Topics in Algebra: Cryptography - Blatt 5

11.30-12:15, Seminarraum 9, Oskar-Morgenstern-Platz 1, 2.Stock

`http://www.mat.univie.ac.at/~gagt/crypto2018`

Goulnara Arzhantseva
goulnara.arzhantseva@univie.ac.at

Martin Finn-Sell
martin.finn-sell@univie.ac.at

1 Test questions from the lecture to refresh:

Question 1.

1. What if in the argument showing that the Existential forgery is always possible we first choose an arbitrary x and then compute the corresponding signature y?
2. Assume that the hash function is not collision-resistant. Is an Existential forgery using a known message attack possible?

Question 2. Why is the ElGamal signature scheme not just the use of the ElGamal cryptosysytem in the DSS? Compare with the RSA signature scheme.

Question 3. Does the ElGamal Signature scheme provide the authentication? Compare to the ECDSA.

2 Exercises

Question 4. Is a collision-resistant hash function always a one way function?

Question 5. Let r be a random number used in the ElGamal Signature scheme.

1. Could we forge the signature if r is made public?
2. Could we forge the signature if we use same r to sign two different messages?
3. In the case of a positive answer, make precise the type of forgery.

Question 6. Under the ECDSA, show that a signature will be accepted by the verifier (i.e. that the verification step is correct).